

6 בפברואר 2019
א' אדר א תשע"ט
סימוכין: ב-ס-844

מסרוני סחיטה

תקציר



ביממה האחרונה מתקבלות ב-CERT הלאומי פניות רבות מאזרחים, אשר מדווחים כי קיבלו מסרון עם הודעת סחיטה. כלל ההודעות נשלחו מאותו הנמען בשם Quagmire, וניסוחן זהה. מההודעה עולה כי התוקף הצליח לפרוץ למכשיר המשתמש וכי ברשותו תצלומים אינטימיים שלו. במידה והמשתמש אינו מעוניין שהתצלומים יפורסמו בפומבי, הוא נדרש להעביר דמי כופרה תוך 72 שעות.

פירוט



החל מאתמול (5/2/2018) נשלחו הודעות אלה לעשרות אלפי אזרחים בישראל. ההודעות נשלחות מאותו הנמען, ותוכנן זהה: תחילה טוען התוקף כי פרץ למכשיר הפלאפון של האזרח, ולאחר מכן מגיע שלב הסחיטה. התוקף מאיים על המשתמש שיפרסם תכנים אינטימיים שלו, במידה ולא ישלם את דמי הכופרה. האימונים נוגעים להפצת סרטון של המשתמש כשהוא צופה בתכנים פורנוגרפיים. את דמי הכופרה, על המשתמש לשלם באמצעות ביטקוין.



ניתן לשתף מידע המסווג "לבן" עם כל קבוצת נמענים, לרבות ערוצים פומביים

חשוב להדגיש כי מדובר בקמפיין רחב היקף ולא בתקיפה ממוקדת מול אזרחים.

פעמים רבות מאגרי מידע (databases) של אתרים, הכוללים שמות משתמש, מספרי טלפון, סיסמאות וכתובות דוא"ל, מודלפים ברשת. תוקפים מנצלים את ההדלפות הללו לטובת הפחדת משתמשים תמימים. לכן, על-אף שהתוקף טוען כי הצליח להשיג תכנים אינטימיים של המשתמש, לרוב מדובר באיום סרק ובפועל התוקף לא פרץ למכשיר המשתמש.

מבירור מול משטרת ישראל, האירוע מוכר גם על ידם ונעשה ניסיון לטפל בבעיה מהשורש, על כן אין צורך להמשיך ולהגיש תלונות במשטרה. כמו כן, מבדיקה שביצעה משטרת ישראל, עד כה אף אזרח לא העביר כספים לארנק הביטקוין המופיע בהודעה.

המלצות



- מומלץ שלא להעביר לתוקף את דמי הכופרה. כאמור, לרוב אין לתוקף אחיזה אמיתית במכשיר, ואף לא ניתן לדעת האם לאחר העברת הכספים הוא יעמוד בהבטחתו.
- במידה שהתוקף מוכיח כי בידיו תכנים אינטימיים, יש לפנות לתחנת המשטרה הקרובה ולהגיש תלונה.
- במידה שמדובר בתכנים אינטימיים של קטינים, אנא פנו למוקד מערך מאו"ר - מערך למניעת אלימות ופשיעה נגד ילדים ונוער ברשת - במספר 105.

במידה שבבדיקתכם התגלה ממצא כלשהו, נשמח לקבלת היזון חוזר.

לכל מידע נוסף ניתן לפנות ל-CERT הלאומי.

שיתוף מידע עם CERT הלאומי איננו מחליף חובת דיווח לגוף מנחה כלשהו, במידה שהתגלה צורך כזה



ניתן לשתף מידע המסווג "לבן" עם כל קבוצת נמענים, לרבות ערוצים פומביים